AMY KLOBUCHAR
MINNESOTA

COMMITTEES:
AGRICULTURE, NUTRITION, AND FORESTRY
COMMERCE, SCIENCE, AND TRANSPORTATION
JOINT ECONOMIC COMMITTEE
JUDICIARY
RULES AND ADMINISTRATION

United States Senate

WASHINGTON, DC 20510

October 22, 2019

Scott Algeier
Executive Director
IT-ISAC Elections Industry Special Interest Group
9401 Centreville Road, Suite 104 Manassas, VA 20110

Re: Request for Information on a Crowd-sourced Coordinated Vulnerability Disclosure Program

Thank you for the opportunity to provide feedback on creating a vulnerability disclosure program for voting systems in the United States. As you know, election security is national security, and so it is vital that we make use of widely used cybersecurity best practices and welcome independent good-faith security review of our nation's election systems.

Creating a vulnerability disclosure program for U.S. voting systems could be a significant step forward for election security. However, to be successful it is important that any such program follow best practices that have worked well in other industries. Below are 3 key principles that I believe are fundamental to creating an effective vulnerability program.

1. **To be effective, a vulnerability disclosure program for voting systems must provide clear legal authorization for good-faith security research by the general public.**

The success of any vulnerability program depends on actually receiving reports. The IT-ISAC's accompanying whitepaper on CVD programs[1] describes a program that potentially limits participation to vetted researchers, which would be detrimental to the effectiveness of the program.

Allowing participation from the general public does not require voting system manufacturers to make machines physically available to anyone who asks. Opening the program to the public means that the program should be capable and interested in accepting private vulnerability reports from good-faith actors, whether they used machines provided by the manufacturer or not, without the fear of legal retaliation. For example, the Department of Defense (DoD) provides authorization to the general public to research vulnerabilities on any DoD websites.[2]

---

[1] "Coordinated Vulnerability Disclosure Program White Paper", Elections Industry-Special Interest Group (EI-SIG). 2019. https://docs.wixstatic.com/ugd/b8fa6c_112b6b0bdc764533816b57dfdb3481b9.pdf
[2] "DoD Vulnerability Disclosure Policy". https://hackerone.com/deptofdefense

In its associated Request for Information (RFI)[3], the IT-ISAC asked *"How to ensure that those engaging in a crowd-sourced CVD program are not nefarious actors seeking sensitive information that can then be used in attacks against the elections' infrastructure?"*

Limiting participation on the basis of preventing unvetted people from gaining information would necessarily require placing restrictions on participating researchers (such as non-disclosure agreements) that would deter many security experts from participating. This may also reflect unrealistic expectations on the part of voting system manufacturers on how tightly information about voting systems used in public elections can reasonably be managed. As in any industry, from a security perspective, it is prudent to assume that the workings of your software and hardware are public knowledge, and to design security controls under that assumption.

Coordinated vulnerability disclosure programs in many sensitive industries allow the general public to safely submit vulnerability reports, even those that make embedded systems or systems not designed to be connected to the internet. For example, medical device manufacturers, car manufacturers, and other companies maintain vulnerability disclosure programs that are generally open to the public,[4] including Philips[5], Dräger[6], and General Motors[7].

2. **To be realistic, a vulnerability disclosure program for voting systems must expect that external security research is always happening and channel that research into effective disclosure.**

Successful vulnerability disclosure programs in industry and in government are designed with the knowledge that the public will always be looking for security issues in their systems, and to incentivize those with good intentions to privately report any issues so they can be promptly fixed before being made public.

In its associated RFI, the IT-ISAC asked *"How best to ensure the confidentiality of the researcher findings so that vulnerability announcements are disclosed simultaneously with a fix or mitigation for the vulnerability?"*

A primary goal of any vulnerability disclosure program is avoiding public disclosure of a vulnerability before a fix or mitigation is available, and experience suggests that security experts who participate in these programs share this goal. However, ensuring that exploitable vulnerabilities are fixed before they can be used to harm the public is ultimately a more important public security goal, and it is not reasonable to attempt to indefinitely restrict public disclosure.

---

[3] "IT-ISAC EI-SIG Request for Information". https://www.it-isac.org/post/it-isac-ei-sig-request-for-information

[4] Coordinated vulnerability disclosure resources. "I Am The Cavalry". https://www.iamthecavalry.org/resources/disclosure-programs/

[5] "Philips coordinated vulnerability disclosure statement" https://www.philips.com/a-w/security/coordinated-vulnerability-disclosure.html

[6] "Dräger Coordinated Disclosure Statement" https://static.draeger.com/security/

[7] "General Motors, Vulnerability Disclosure Program" https://hackerone.com/gm

Many successful vulnerability disclosure programs acknowledge this tension by asking the security expert to agree to a time-limited window for the company to address any reported vulnerability before the security expert makes their report public. For example, the General Services Administration asks for 90 days to patch their systems[8], while Dräger strongly encourages coordinated disclosure without attempting to legally require it[9].

State requirements that voting systems be formally certified can delay the deployment of fixes. At the same time, Election Day cannot be postponed, increasing the pressure to deploy fixes in a timely manner. These competing pressures are serious, and it may be reasonable to establish expectations around public disclosure that are tailored to elections. However, even if challenges like certification delays remain an issue, voting systems manufacturers must work out reasonable, time-limited, and researcher-friendly terms for disclosure.

Ultimately, for a vulnerability disclosure program for voting systems to be the most effective at convincing security experts to contact voting systems manufacturers, it should grant clear legal authorization for good-faith security research, without requiring security experts to agree to permanent confidentiality agreements.

3. **To be complete, a vulnerability disclosure program for voting systems must include their manufacturers' own websites and corporate information systems.**

The safety of any voting system also depends on the security of the systems that are used to design and develop that system. At minimum, any company that makes software or firmware must make sure that its source code is not changed by malicious actors. This is even more important for makers of proprietary software, since changes to proprietary source code are not publicly auditable.

In its associated RFI, the IT-ISAC asked *"How to manage a crowd-sourced CVD program on systems that are designed to be closed, isolated, and disconnected from the Internet including stand-alone embedded systems?"*

Even stand-alone embedded systems that may be disconnected from the internet rely on their supply chain remaining intact. If a member of the public finds a vulnerability on a public website run by a voting system manufacturer, this could have unexpected ramifications, particularly if that website is hosted on a server inside a trusted environment. Even seemingly small vulnerabilities, such as defacement, could be used by attackers as part of a campaign to phish staff and compromise an organization.

Voting system manufacturers should acknowledge this by welcoming vulnerability reports that apply to all of their internet-accessible IT systems, including systems not intentionally made internet-accessible.

[8] "Vulnerability disclosure policy". https://18f.gsa.gov/vulnerability-disclosure-policy/
[9] "Dräger Coordinated Disclosure Statement". https://static.draeger.com/security/

In summary, I recommend that any vulnerability disclosure program created by voting system manufacturers:

- Provide clear reporting channels and legal authorization for good-faith security research by the general public.
- Establish reasonable, time-limited, and researcher-friendly expectations around public disclosure.
- Apply to any internet-accessible system operated by the voting system manufacturer, not only the voting systems themselves.

Thank you again for the opportunity to provide feedback on this initiative.

Amy Klobuchar
United States Senator